How to Create a Domain Controller

Overview

The purpose of this guide is to show you how to secure your network and improve its management capabilities by implementing a domain-based network infrastructure (manually and through PowerShell). First, I will show you how to promote a Windows Server to a Domain Controller. Then, I will show you how join a Windows PC to your new domain, and finish by showing you how to build an efficient file-sharing environment by creating and combining a File Share, a Security Group, a GPO and a Mapped Drive.

Prerequisites

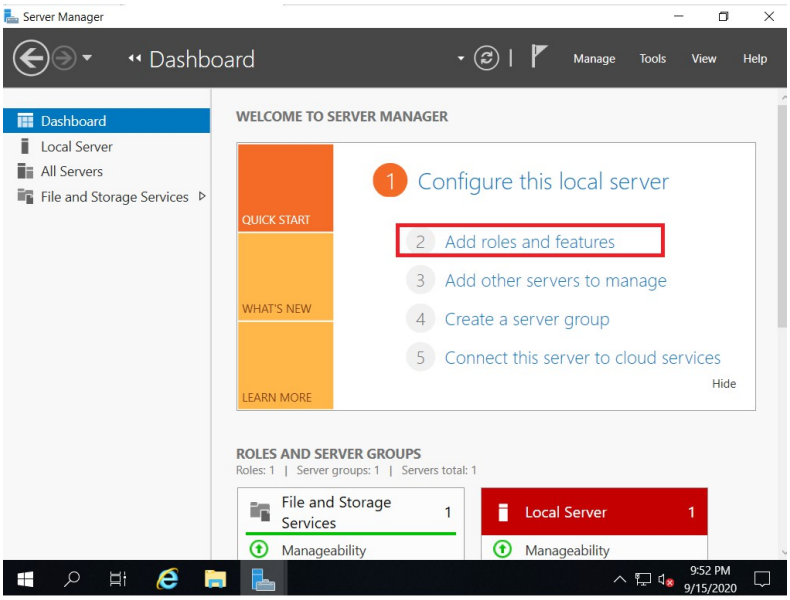
- One Windows server with a static address
- One Windows PC

Contents

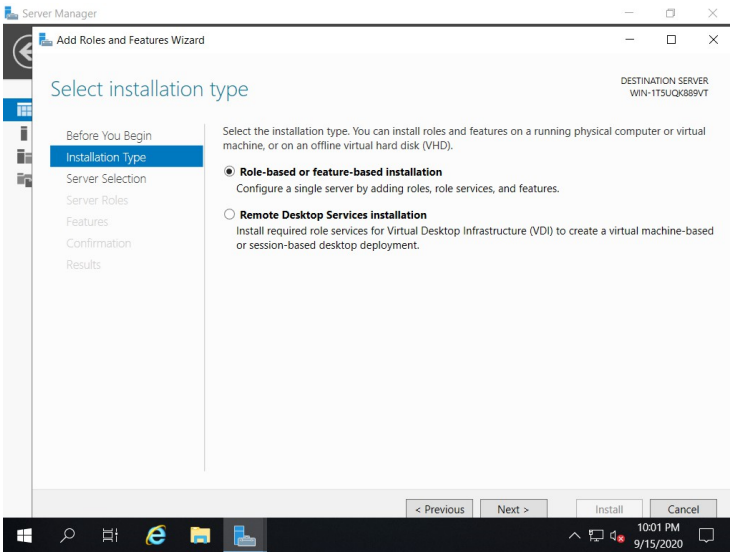
How to Turn Your Windows Server into a Domain Controller

Step 1. Log on to the server as an administrator.

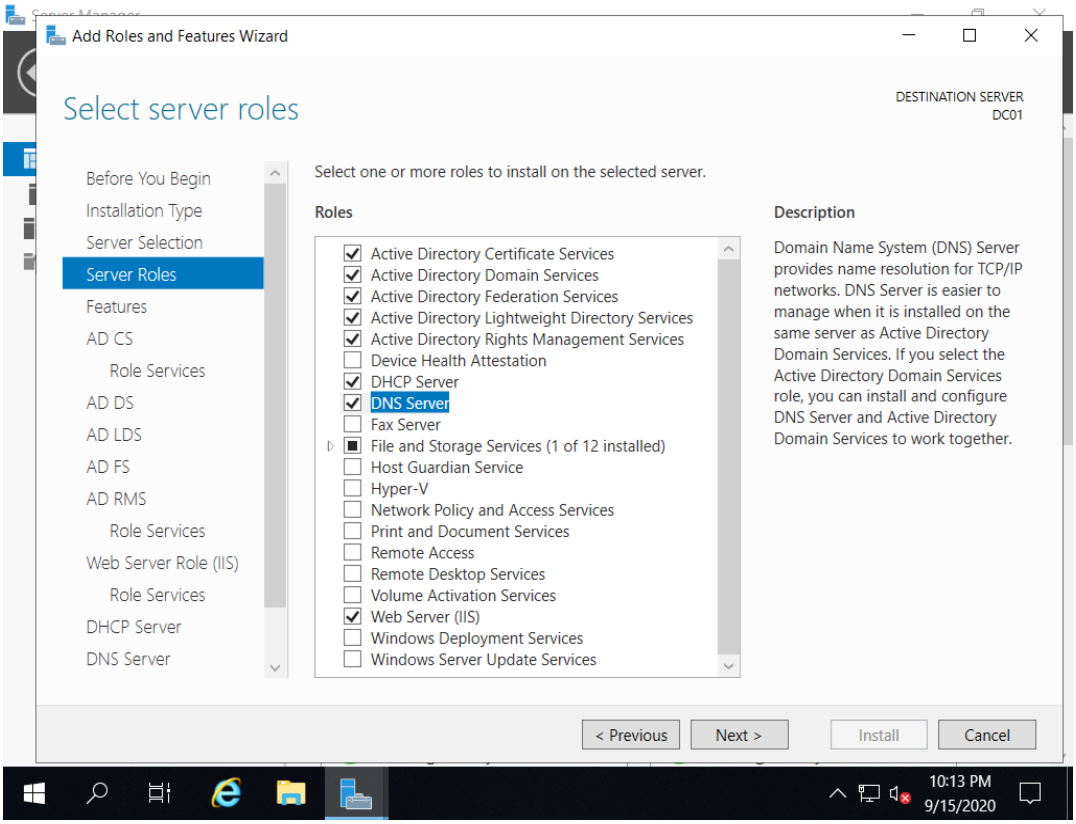
Step 2. Open Server Manager and click the “Add roles and features” button on the right side of the screen.



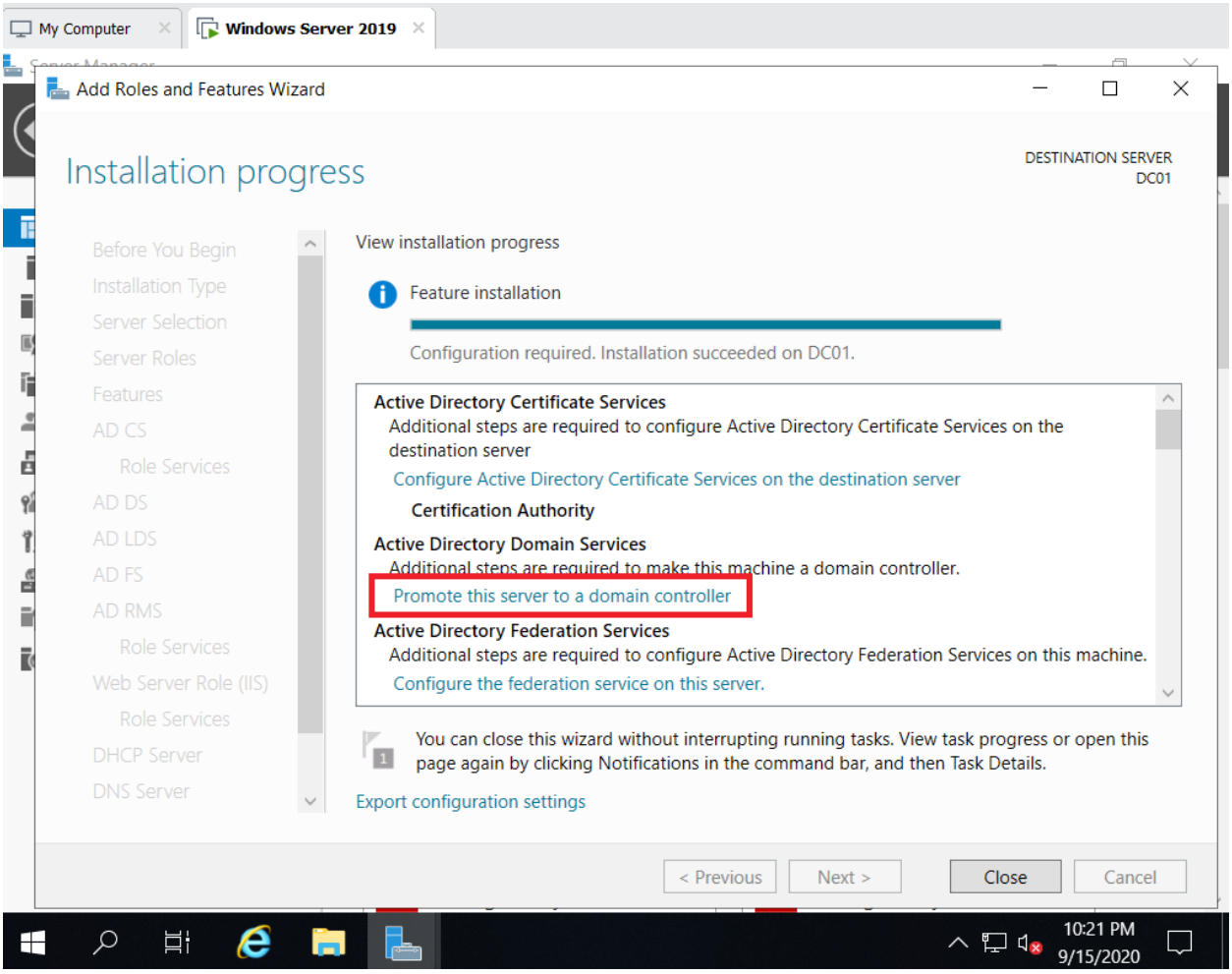
Step 3. Select “Role-based or feature-based installation.”



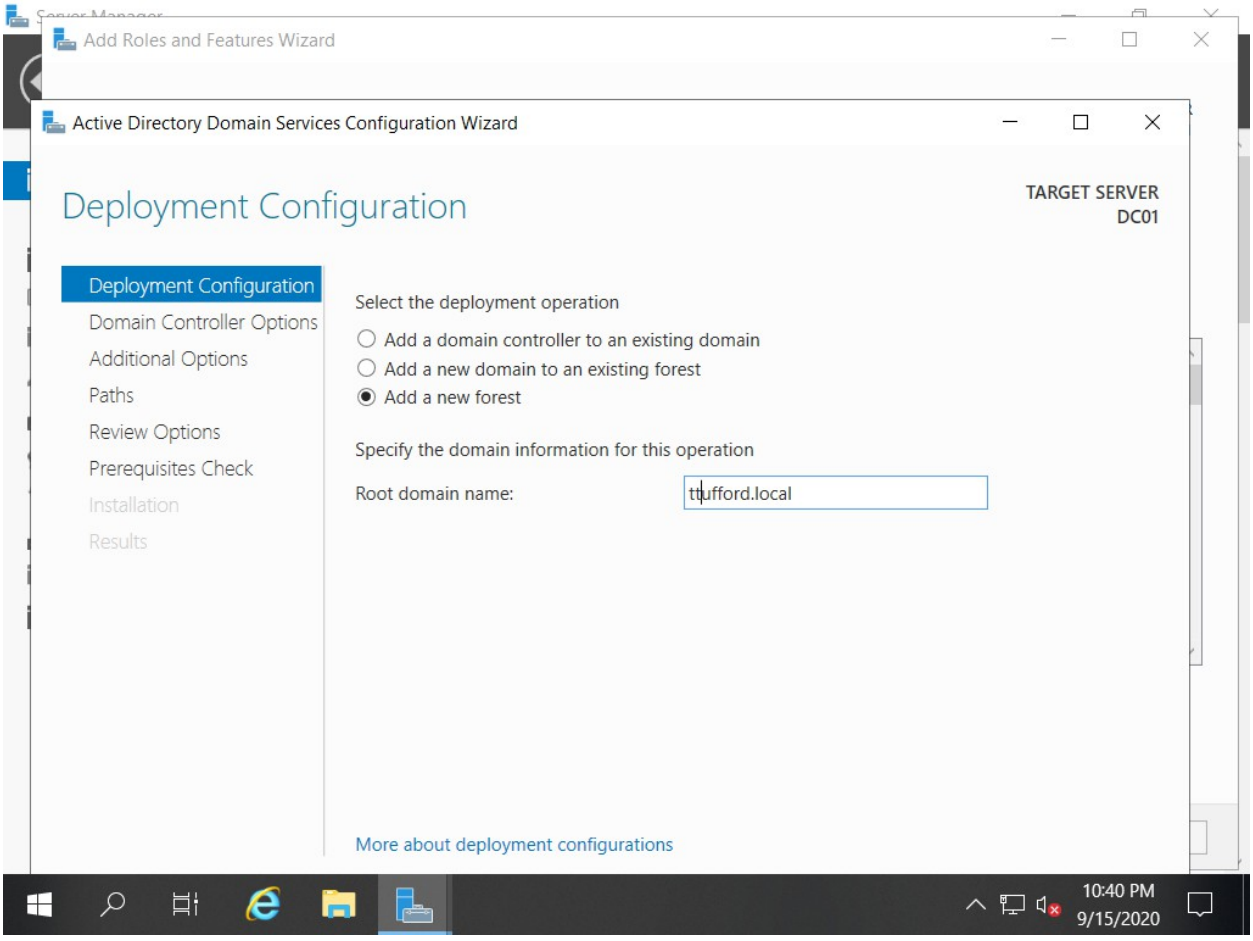
Step 4. Select the roles in the image below, then press next.



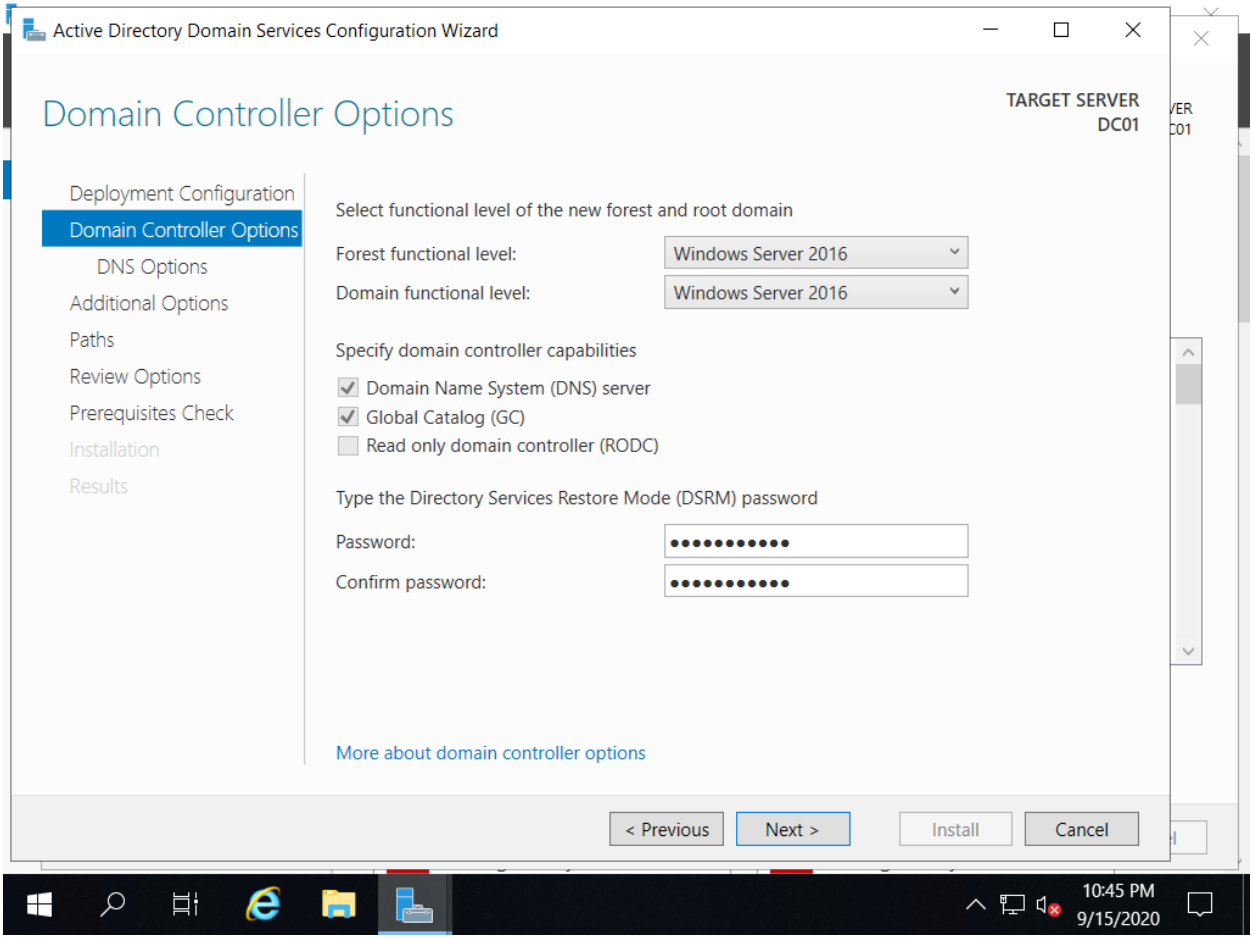
Step 5. Wait for the features to install, then click the option to “Promote this server to a Domain Controller.”



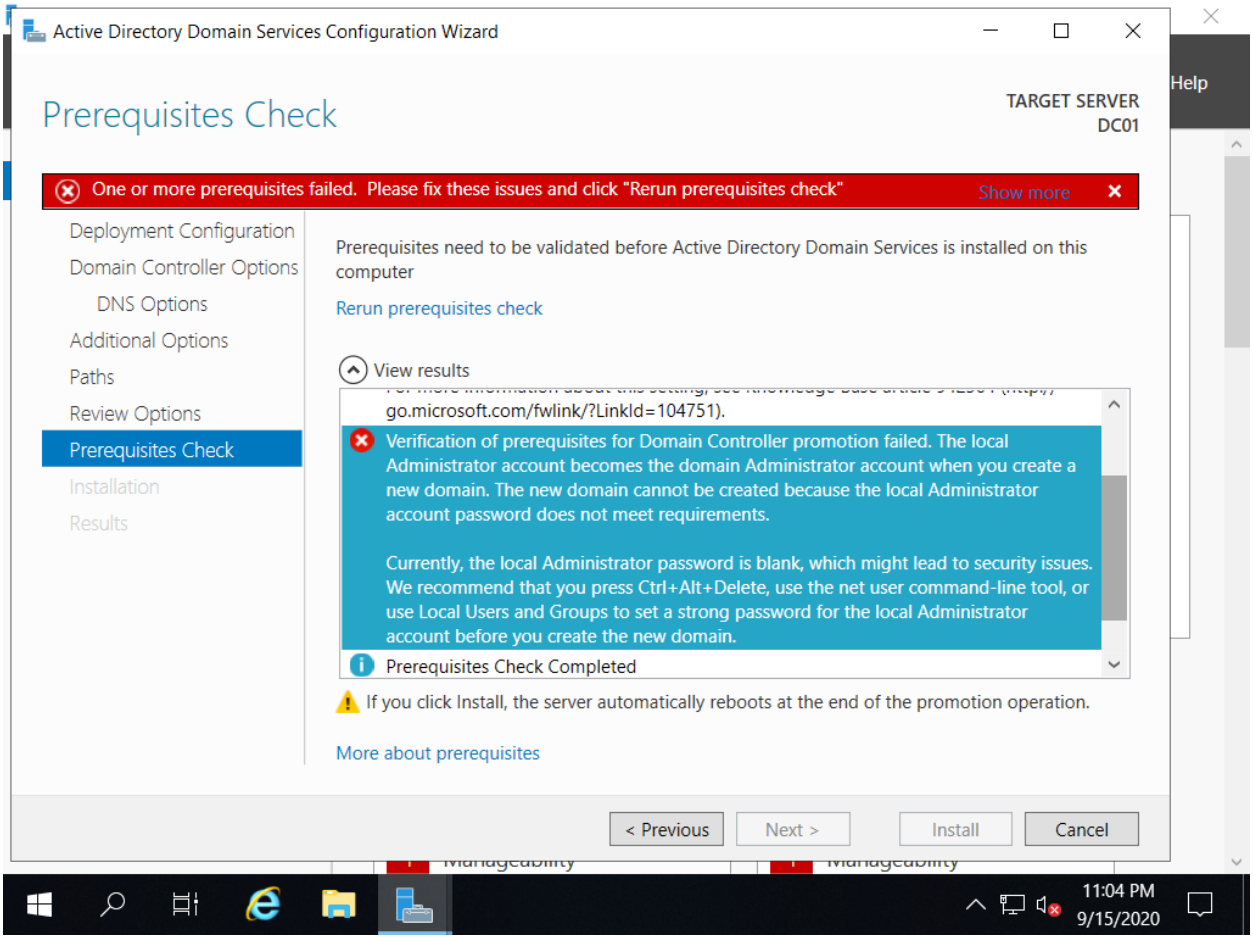
Step 6. Next, you will be directed to the “Active Directory Domain Services Configuration” wizard. Type the name of your domain in the “Root domain name” box on the bottom, then press next.



Step 7. Then, specify “DNS” and “GC” capabilities by checking the boxes. Afterward, you will be asked to enter your password and press next.



Step 8. Next, you will be taken to the “Prerequisites Check” section. You might not be able to proceed until you do a bit of troubleshooting. The result below states that I do not have a password under my administrator account.



Step 9. If you had the exact same error:

a. Go to the Control Panel.

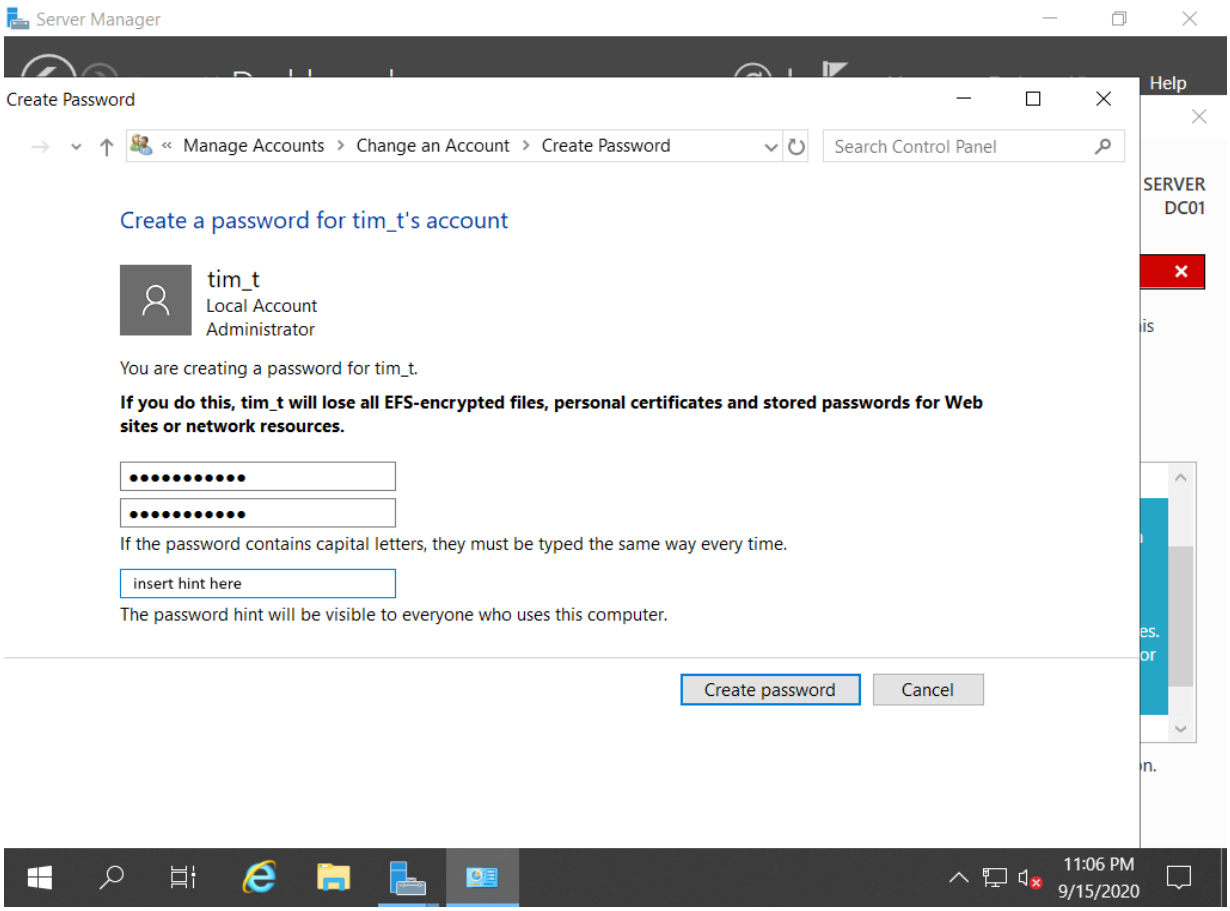
b. Click “Manage Accounts.”

c. Click “Change an Account.”

d. Then, click “Create Password.”

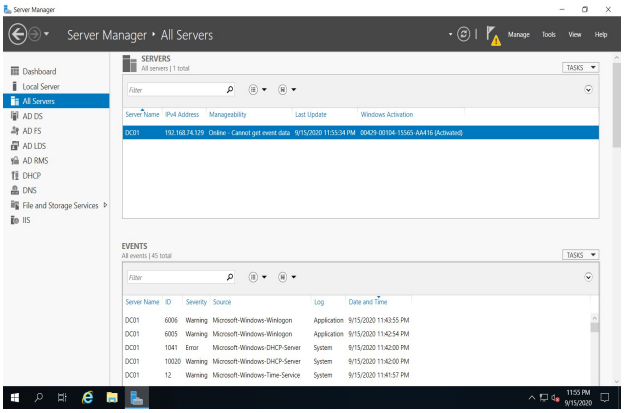
e. Enter a password then click OK.

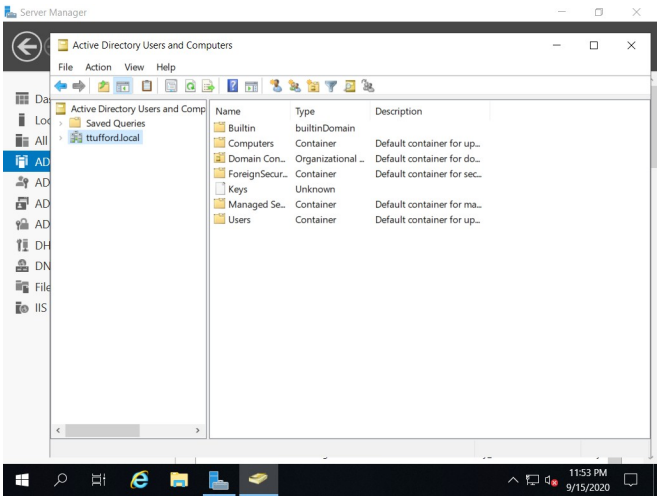
I also had to restart the server for the changes to take place. Afterward, I was able to pass the prerequisite test.



Step 10. Validate that you can open the installed services.

Below are screen shots of “Server and Events” and “Active Directory Users and Computers.”





How to Turn Your Windows Server into a Domain Controller (with PowerShell)

```
#PowerShell script for AD DS Deployment


#!!!!! Your device will reboot after you run this script !!!!!

Import-Module ServerManager

# Define which features to install
$featuresToCheck = @('AD-Domain-Services', 'AD-Certificate', 'AD-Federation-Services',
'DHCP', 'DNS', 'Web-Server')

#Check and install each feature
foreach($feature in $featuresToCheck){
    $featureStatus = Get-WindowsFeature -Name $feature
    if(-not $featureStatus.Installed){
        Write-Host "Installing $feature..."
        try{
            Install-WindowsFeature -Name $feature -IncludeManagementTools -ErrorAction
Stop
            Write-Host "$feature installed successfully"
        }
        catch{
            Write-Host "Failed to install $feature"
        }
    }
    else{
        Write-Host "$feature is already installed."
    }
}

#Prompt the user for a Domain Name and a Netbios Name
$domainName = Read-Host "Please enter the Domain Name (e.g., example.com): "
$domainNetbiosName = Read-Host "Please enter the Netbios Name (short name for the
domain): "

#Import ADDSDeployment module and install AD DS Forest
Import-Module ADDSDeployment
try {
    Install-ADDSForest `
    -CreateDnsDelegation:$false `
    -DatabasePath "C:\Windows\NTDS" `
    -DomainMode "WinThreshold" `
    -DomainName $domainName `
    -DomainNetbiosName $domainNetbiosName `
    -ForestMode "WinThreshold" `
    -InstallDns:$true `
    -LogPath "C:\Windows\NTDS" `
    -NoRebootOnCompletion:$false `
    -SysvolPath "C:\Windows\SYSVOL" `
    -Force:$true
}
catch {
    Write-Host "Failed to install AD DS Forest: $_"
}
```

How to Join a Windows PC to Your Domain

Step 1. First, do the following to get the IP of your domain controller:

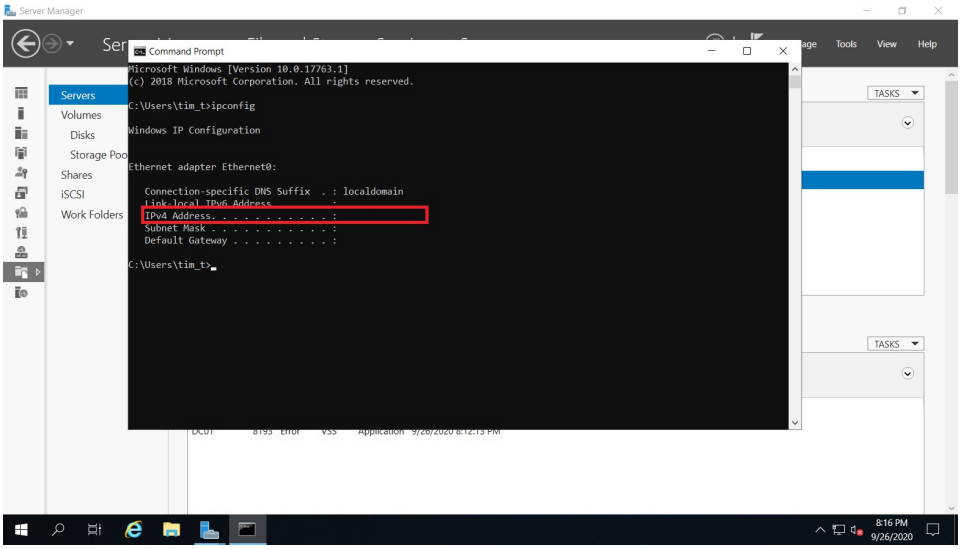
a. Log in to your domain controller.

b. Open the Command Prompt.

c. Type ipconfig.

d. Press enter.

e. Take note of the IPv4 Address.



Note: Your server needs to stay turned on for the rest of these steps to work.

Step 2. Next, make the domain controller's IP your PC's “Preferred DNS Server” by doing the following:

a. Log in to your Windows PC.

b. Then, open the Control Panel.

c. Click “Network and Internet.”

d. Click “Network and Sharing Center.”

e. Click “Network Settings.”

f. Then, click on “Ethernet0.”

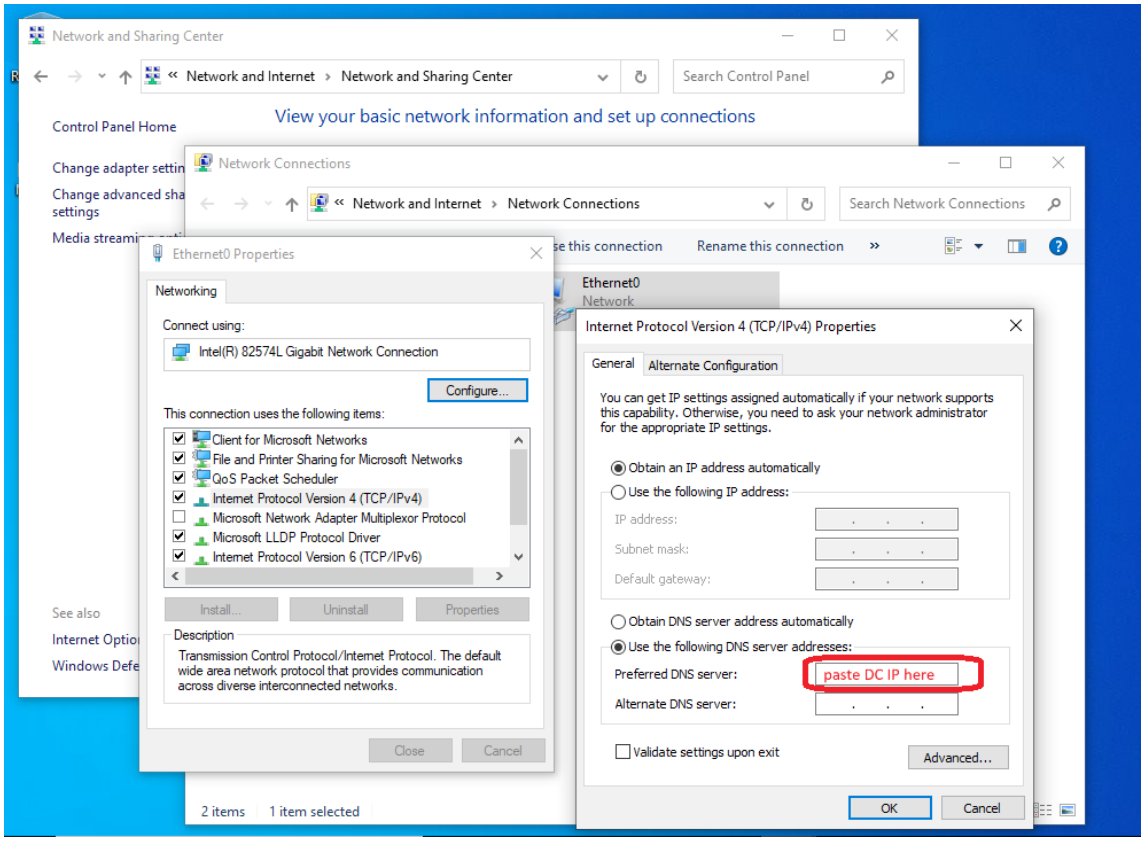
g. Next, right click.

h. Select Properties.

i. Click “IPV4.”

j. Select Properties again.

k. Then, type the IP from Step 1 into the “Preferred DNS Server” field like so:



Step 3. Make your PC a member of your domain by doing the following:

a. Open the Control Panel.

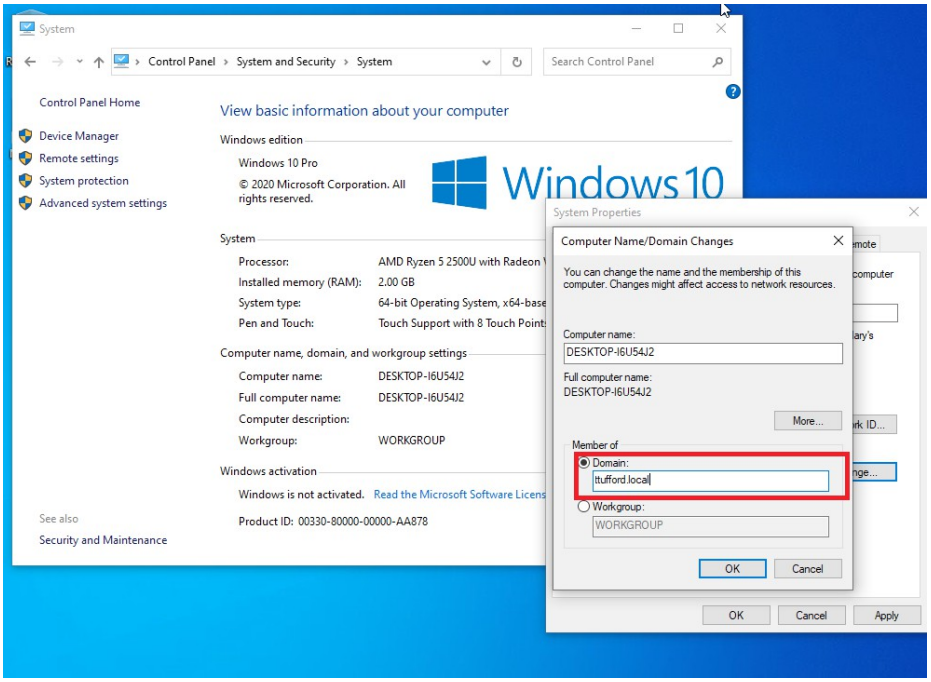
b. Select “System and Security.”

c. Click “System.”

d. Click “System Properties.”

e. Then, click “Change.”

f. In the resultant window, type the name of your domain into the “Domain” field. You will be asked to restart afterward.



Step 4. Open PowerShell, then run the following command to validate whether or not this device has been joined to the domain: ipconfig/all.

```
PS C:\Users\tuffo> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : DESKTOP-I6U54J2
   Primary Dns Suffix  . . . . . . . : ttufford.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : ttufford.local
                                       localdomain
```

Step 5. Validate that the client is now visible in Active Directory Users and Computers (ADUC) by doing the following:

a. Log back in to your Domain Controller and open the Start Menu.

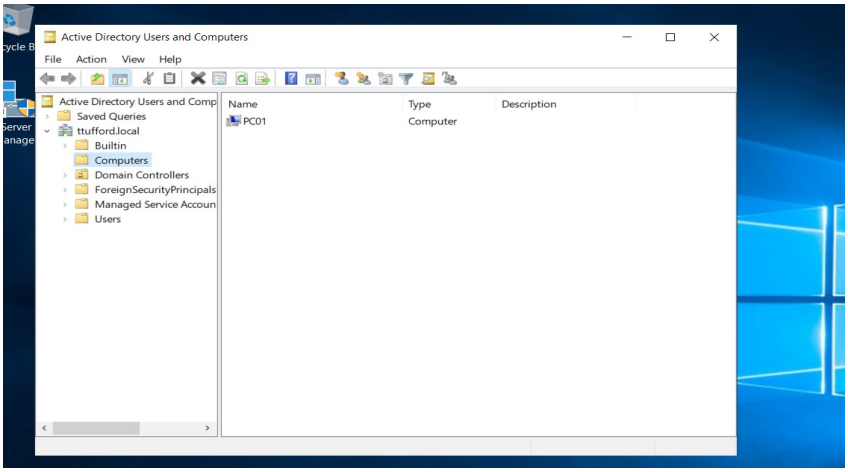
b. Then, open “Active Directory Users and Computers.”

c. Select your domain in the left pane of the ADUC window (ie. tufford.local).

d. Collapse the domain by clicking the arrow next to it.

e. Click the “Computers” directory beneath your domain.

f. If your PC appears on the right side of the page, then it has successfully joined the domain.



How to Join a Windows PC to Your Domain (with PowerShell)

```
#PowerShell script that joins a Windows PC to a domain


#!!!!! This device will restart after this script has finished running !!!!!

#Prompt for domain name, username and password
$yourDomain = Read-Host "Please enter your domain name: "
$yourUsername = Read-Host "Please enter your username: "
do{
    $yourPassword = Read-Host "Please enter your password (minimum 8 characters): "

    #Check password length
    if ($yourPassword.Length -lt 8){
        Write-Host "Error: Password must be at least 8 characters long."
-ForegroundColor Red
    }
}
while ($yourPassword.Length -lt 8)

$domain = $yourDomain
$username = "$yourDomain\$yourUsername"
$password = $yourPassword
$credential = New-Object System.Management.Automation.PSCredential($username,
(ConvertTo-SecureString $password -AsPlainText -Force))

#Join the computer to the domainafter a successful ping
try{
    # Get the domain controller's hostname
    $dc = (Get-ADDomainController -DomainName $domain -ErrorAction Stop).HostName

    #Ping the domain controller
    if(Test-Connection -ComputerName $dc -Count 2 -ErrorAction Stop) {
        Write-Host "Successfully pinged the domain controller: $dc" -ForegroundColor
Green
        #Join the device, then restart
        Add-Computer -DomainName $domain -Credential $credential -Restart
    }
}
catch{
    Write-Host "Error: Unable to communicate with the domain controller. Ensure that
the domain name is correct and the domain controller is reachable." -ForegroundColor
Red
    Write-Host "Detailed Error: $_" -ForegroundColor Red
}
```

How to Give Your PC Access to a File Share

Create a File Share

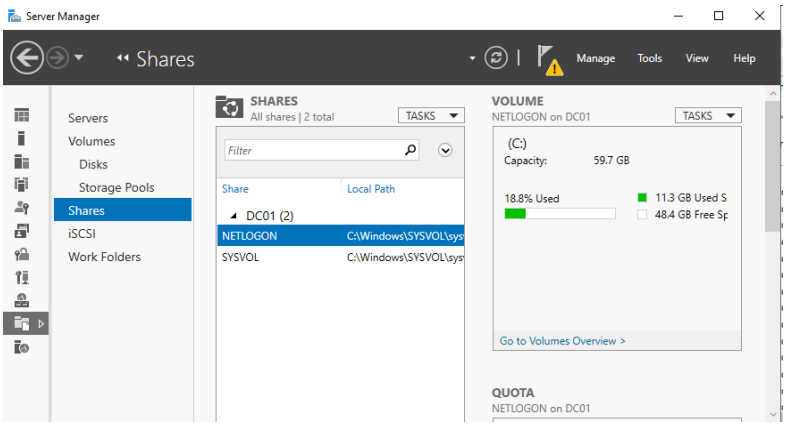
Step 1. Access your Domain Controller's “Shares” by completing the following steps:

a. Log on to your Domain Controller.

b. Open Server Manager.

c. Then, press the “File and Storage Services” button on the left side of the screen. This will redirect you to a new page.

d. When the page loads, click the “Shares” button on the left side of your screen.



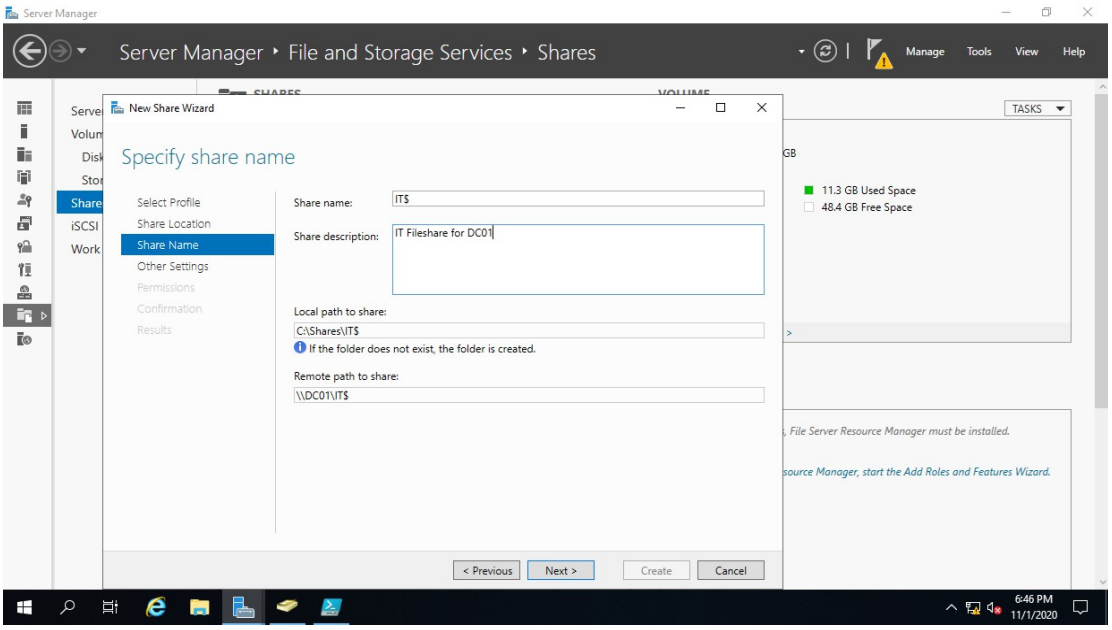
Step 2. Start the process of creating your “Share” by:

a. Right clicking on your domain controller (eg. DC01), and selecting “New share.” This will launch the “New Share Wizard.”

b. Select “SMB Share - Quick” to create a Server Message Block (SMB) share.

c. Then, specify where you want your “Share Location” to be. For simplicity, I chose the “Select by volume” option.

d. When you are asked to specify the “Share name,” give it a “Share name,” “Share description,” “Local path” and “Remote path,” like so:



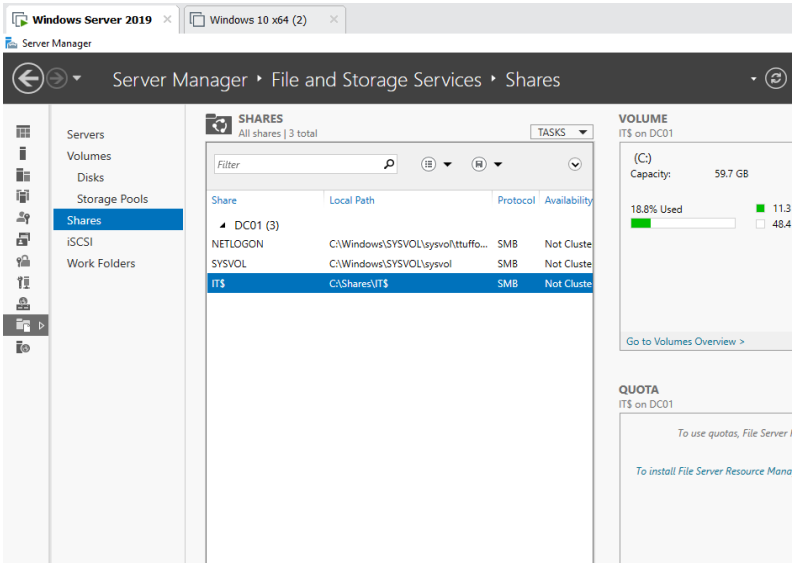
e. Press next. You will then be directed to the “Other Settings” page.

f. Use the default settings, then press Next. This will direct you to the “Permissions” page.

g. Use the default permissions for now, then press Next again. You will then be directed to the “Confirmation” page.

h. If you are satisfied with the settings you have made, press Next. You will then be taken to the “Results” page.

i. Press OK. Ensure that you can now see your newly created File Share in your list of “Shares,” like so:



Create a Security Group

Step 3. Create a Security Group in an Organizational Unit by:

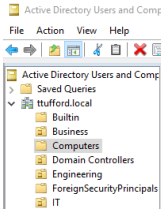
a. Opening “Active Directory Users and Computers” (ADUC).

b. Then, select your domain in the left pane of the ADUC window (ie. ttufford.local).

c. Collapse the domain by clicking the arrow next to it.

d. Create a new Organizational Unit (OU) by right-clicking on the domain, selecting “New,” then pressing “Organizational Unit.”

e. Give it a name, then press enter; your OU should now be visible. I named mine “IT.”



f. Right click on the OU you just created, select “New,” then press “Group.”

g. Give it a Name; I called mine “ShareGroup.”

h. For “Group scope,” choose “Global.”

i. For “Group type,” select “Security.”

j. Click OK.

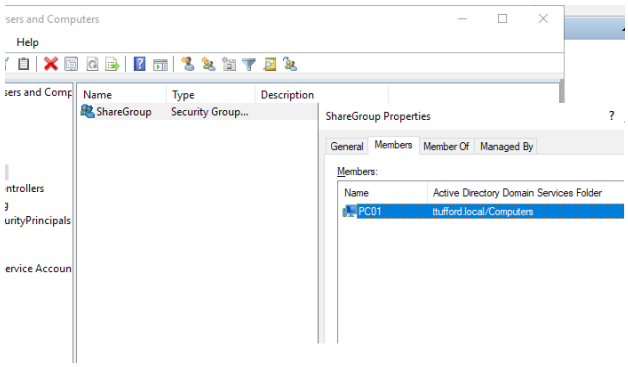
Step 4. Add Your PC to this new group by:

a. Right-clicking on the group you just created and selecting “Properties.” A new menu will open.

b. Navigate to the “Members tab” at the top.

c. Click “Add.”

d. Select your PC's host name in the resultant window, then press OK. I picked PC01.



Create a GPO that Links to Your Security Group

Step 5. Create a GPO called “Share” by:

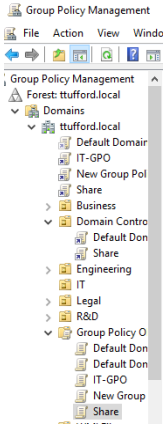
a. Opening the Group Policy Management Console (GPMC).

b. In the left pane, navigate to the “Group Policy Objects” node beneath your domain.

c. Right-click on “Group Policy Objects” and select “New.”

d. In the dialog that appears, name the new GPO; I called mine "Share."

e. Click OK to create the GPO.



Step 6. Next, tie the GPO to the group you created in step 4 by:

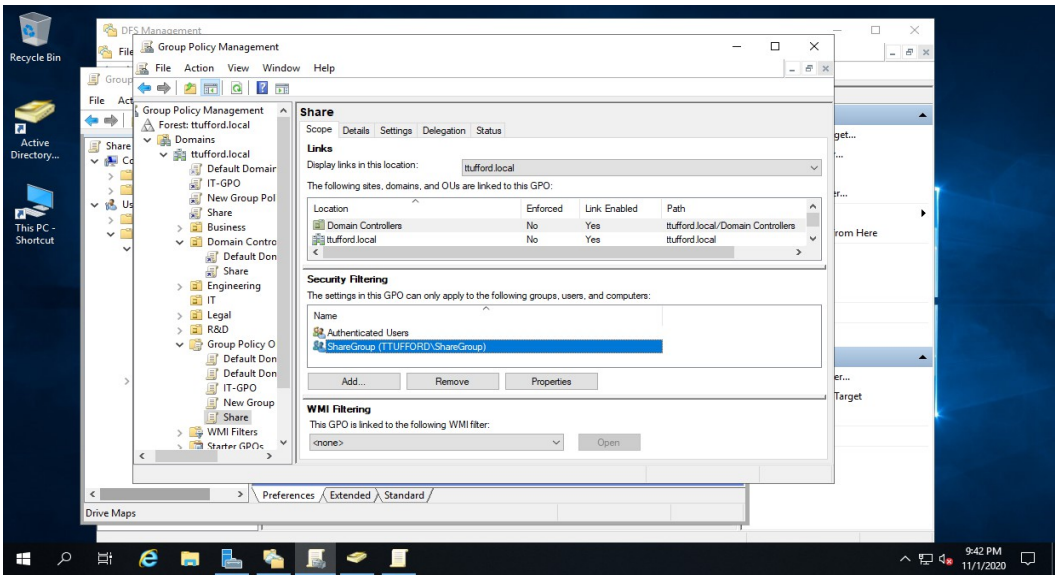
a. Selecting the "Share" GPO you just created.

b. In the right pane, under the “Scope” tab, find the “Security Filtering” section.

c. Then, click on the “Add” button to add the Security Group you made earlier (ie. “ShareGroup”).

d. Name the filter: “ShareGroup,” then click “Check Names” to verify it exists.

e. Click OK once it has been verified.



k. By default, this GPO will include the "Authenticated Users" group. If you want to restrict it only to the members in the "ShareGroup" group, you must remove the "Authenticated Users" filter. You can do this by clicking on “Authenticated Users,” and clicking the “Remove” button.

Map a Network Drive to Your File Share & Apply it to Your GPO

Step 7. To map a network drive to your File Share:

a. In GPMC, search for the “User Configuration” node.

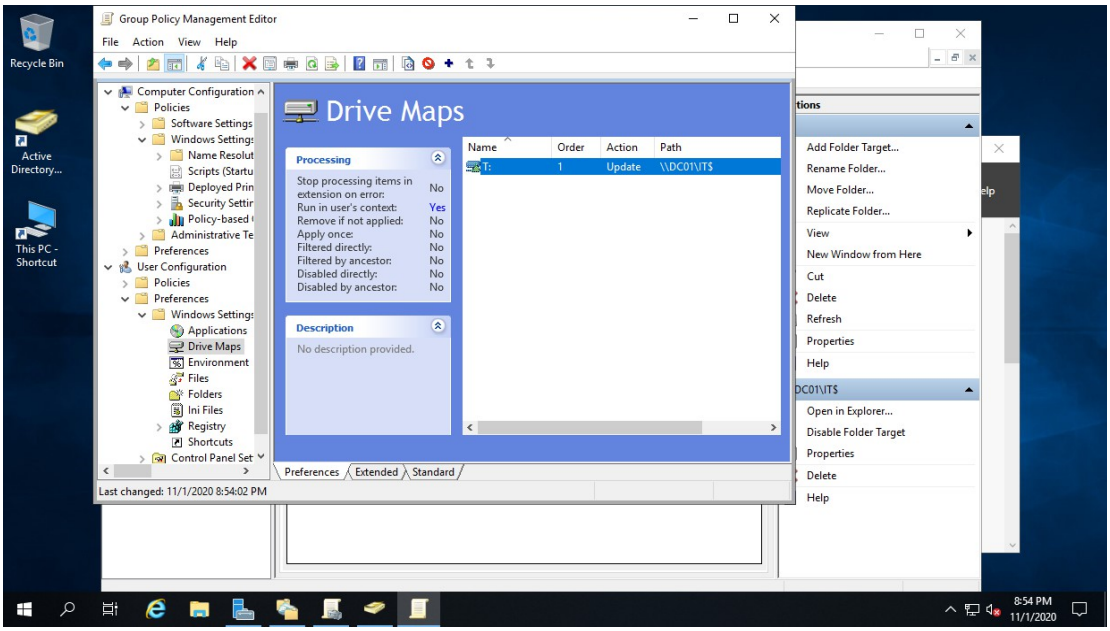
b. Click “Preferences.”

c. Then, click “Windows Settings.”

d. Right Click “Drive Maps,” then press “New Mapped Drive.”

e. Then specify the path of the shared folder you previously configured.

f. Next, match it to a drive of your choice. I chose the T:/ drive.



Step 8. Next, redirect your folder to your Share by doing the following:

a. Go back to the GPO you made in the GPMC.

b. Right click on it, then press “Edit.”

c. Once it takes you to a new screen, go to “User Configuration.”

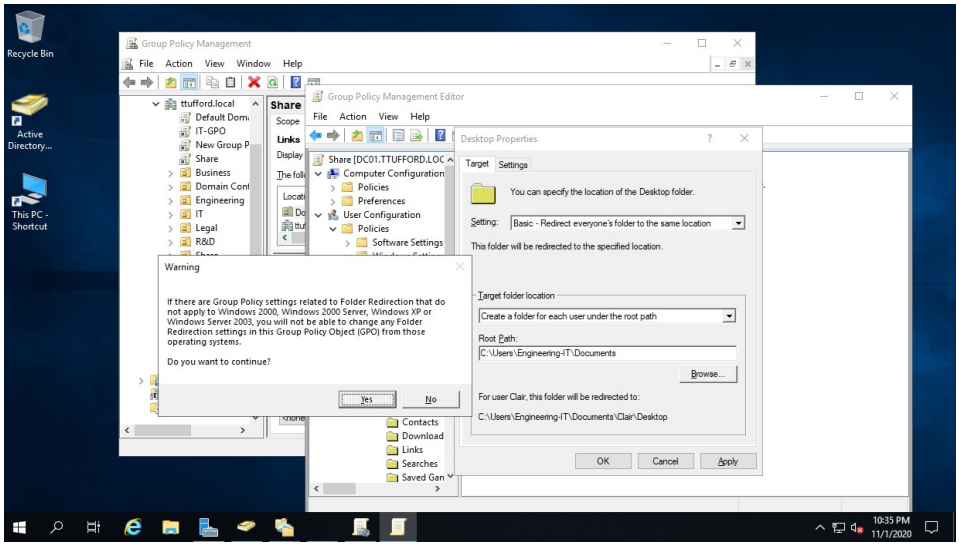
d. Click “Policies.”

e. Then, click “Windows Settings.”

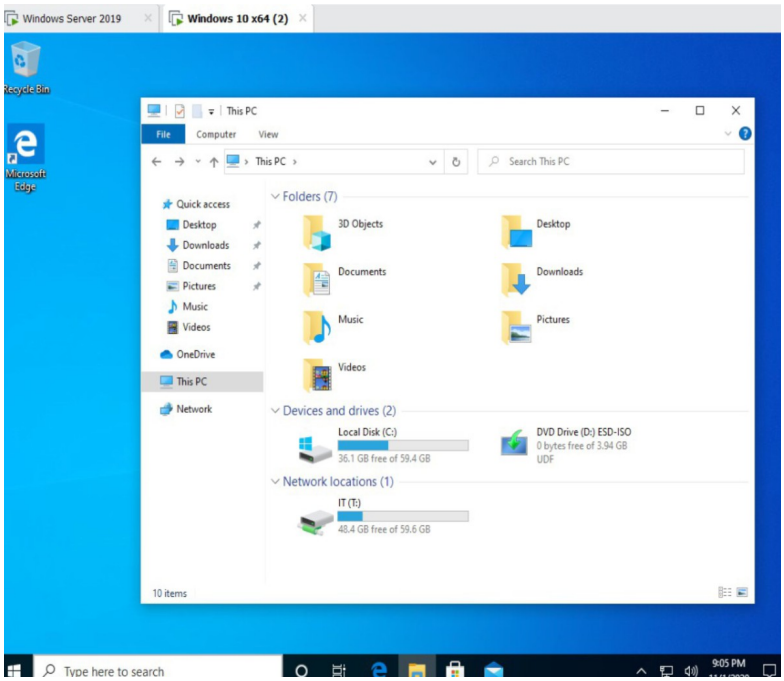
f. Next, click “Folder Redirection.”

g. Right click on “Documents,” then click “Basic setup.”

h. Finally, enter the path to your share.



Step 9. Validate that the T:/ drive is now visible in your “Network locations” when you log into PC01. If you are not able to see the drive, you can force an update on your device by running gpupdate /force in the Command Prompt.



How to Give Your PC Access to a File Share (with PowerShell)

```
#Prompt user for various inputs
$domain = Read-Host -Prompt "Enter the domain"
$gpoName = Read-Host -Prompt "Enter the GPO Name (default: Share)" -Default "Share"
$securityGroupName = Read-Host -Prompt "Enter the Security Group Name (default:
ShareGroup)" -Default "ShareGroup"
$organizationalUnitName = Read-Host -Prompt "Enter the Organizational Unit Name
(default: IT)" -Default "IT"
$pcName = Read-Host -Prompt "Enter the Name of the Computer to be added to your OU
(default: PC01)" -Default "PC01"
$shareName = Read-Host -Prompt "Enter the Share Name (default: MyFileShare)" -Default
"MyFileShare"
$sharePath = "C:\Shares\$shareName"
$driveLetter = Read-Host -Prompt "Enter the Drive Letter (default: T:)" -Default "T:"
$folderRedirectionPath = "\\$env:COMPUTERNAME\$shareName"

#Create the Share directory
if(-Not (Test-Path $sharePath)){
    New-Item -ItemType Directory -Path $sharePath
}

#Create the File Share
New-SmbShare -Name $shareName -Path $sharePath -FullAccess "Everyone"

#Create an Organizational Unit
New-ADOrganizationalUnit -Name $organizationalUnitName -Path "OU=Users,$domain"

#Create the Security Group
New-ADGroup -Name $securityGroupName -GroupScope Global -GroupCategory Security -Path
"OU=$organizationalUnitName,OU=Users,$domain"

#Add computer to the Security Group
Add-ADGroupMember -Identity $securityGroupName -Members $pcName

#Create a new GPO
$gpo = New-GPO -Name $gpoName

#Link GPO to the domain
New-GPLink -Name $gpoName -Target "DC=$domain,DC=com"

#Add Security Filtering to GPO
Set-GPPermission -Name $gpoName -TargetName $securityGroupName -TargetType Group
-PermissionLevel GpoApply

#Remove Authenticated Users from the GPO
Remove-GPPermission -Name $gpoName -TargetName "Authenticated Users" -TargetType Group
-RemovePermissionLevel GpoApply

#Configure Mapped Drive in GPO
$driveMap = @{"Action" = "Create"; "DriveLetter" = $driveLetter; "Path" =
$folderRedirectionPath}
Set-GPRegistryValue -Name $gpoName -Key
"HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive" -ValueName
"Network Location" -Value $driveMap

#Configure Folder Redirection in GPO
$folderRedirection = @{
    "Documents" = $folderRedirectionPath
}
foreach($folder in $folderRedirection.Keys){
    New-GPRegistryValue -Name $gpoName -Key
"HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\State" -ValueName
"$folder" -Value $folderRedirection[$folder]
}
```